UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
	)	
	)	
v.	)	Criminal No. 14-CR-40028-TSH
	)	
JAMES MERRILL,	)	
Defendant		

Defendant James Merrill's Motion to Suppress Evidence and Incorporated Memorandum of Law

Now comes the Defendant, James Merrill, by and through undersigned counsel, pursuant to the Fourth Amendment of the United States Constitution and Rule 12 of the Federal Rules of Criminal Procedure, and respectfully moves the Court for an order suppressing all evidence seized pursuant to the execution of a search warrant for James Merrill's personal email account, Jim-Merrill@comcast.net, as the search warrant was unconstitutionally overbroad and unparticularized.

The search warrant at issue permitted agents to: (1) seize the entire content of James Merrill's personal email account without limitation, including all personal email, personal pictures, and personal videos, and without any date restriction; and (2) execute a search protocol across the entire data set for various categories of records for the date range October 1, 2012, through September 25, 2014, which extended well beyond the period of the alleged criminal conduct. Because the warrant did not limit the seizures to the date range of the alleged fraudulent scheme and avoid search categories likely to turn up information of the most personal and sensitive nature, the warrant was unconstitutionally overbroad and lacking in particularity. In addition, because the warrant was so obviously overbroad and lacking in particularity, it was invalid on its face and no reasonable law enforcement officer could have relied on its validity,

thus depriving the government of the "good faith" safe harbor. For these reasons, and others detailed *infra*, all evidence seized pursuant to the search warrant must be suppressed.

As further grounds and reasons therefore, Mr. Merrill relies upon the memorandum of law set forth below.

Memorandum of Law

I. *Facts.*

A. The Search Warrant.

The search warrant for Mr. Merrill's email account was issued on September 25, 2014, over four months after the arrest of Mr. Merrill on a federal criminal complaint and two months after a federal indictment was returned. *See* Search Warrant attached hereto as Exhibit 1; Application For A Search Warrant, attached hereto as Exhibit 2; Affidavit of John S. Soares in Support of Search Warrants ("Affidavit," "Soares' Affidavit," or "Email Affidavit" herein), attached hereto as Exhibit 3. The face of the email search warrant authorized law enforcement to seize the following materials from Mr. Merrill's personal email account at Jim-Merrill@comcast.net:

> "Evidence, fruits, or instrumentalities of violations of 18 U.S.C. §1349, conspiracy to commit wire fraud, and 18 U.S.C. §1343, wire fraud. The items to be seized are detailed in Attachment B hereto."

Exhibit 1. Categories I and II of Attachments B directed Comcast Communications LLC to create and provide to law enforcement "an exact electronic duplicate of" James Merrill's entire email account, including, among other items, all email, texts, instant messages, calendar data, contacts, and electronic data files, including images and videos. Exhibit 1. Category III of Attachment B provided a search protocol for law enforcement that provided: "A. Evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1349

and 18 U.S.C. § 1343, including records from October 1, 2012 through the present [September 25, 2014] relating to[]" ten individual categories of records and data, including "[t]he contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content . . ." Exhibit 1.

B. Agent Soares' Email Affidavit.

The affidavit submitted in support of the email search warrant was prepared by Special Agent John Soares and articulated essentially the same information outlined in Soares' April 15, 2014, affidavit submitted in support of the TelexFree office search warrant. To avoid unnecessary duplication, instead of summarizing the entirety of Soares' affidavit, the defendant relies upon the summary of facts outlined in his companion pleadings, filed today, and supplements those facts with additional information contained in Soares' email warrant affidavit as follows.

In Soares' email affidavit, he acknowledged that Mr. Merrill and Mr. Wanzeler had been charged criminally in a complaint on May 9, 2014, and were later indicted on July 23, 2014, on charges related to the alleged pyramid scheme. Email Aff. at ¶¶13-14. No other TelexFree employees were charged in the indictment. *See id.* The affidavit also did not establish probable cause against any other individuals and notably the affiant did not allege that any close friends or members of Mr. Merrill's family were in any way involved in the alleged fraudulent scheme. *See* Email Aff.

In his effort to connect Mr. Merrill's personal email account to criminal activity, the affiant identified a total of six emails sent to or from Mr. Merrill's Comcast email address in which TelexFree business was allegedly discussed: (1) a July 30, 2012, email from Mr. Wanzeler discussing changes to the TelexFree compensation structure to help

make the company compliant with the multi-level marketing business model; (2) an August 12, 2012, email from Wanzeler expressing concern that a company with the same lawyers as TelexFree was closed due to an investigation; (3) an August 17, 2012, email from Mr. Merrill telling Mr. Wanzeler that a "lawyer is only as good as the company's ability to follow the lawyer's recommendation;" (4) a November 19, 2013, email from Mr. Merrill's brother with an Excel spreadsheet analyzing TelexFree's business; (5) a December 12, 2013, email confirming a lunch date with a prospective CEO; and (6) a December 26, 2013, email from Mr. Merrill to a TelexFree financial consultant with no description of the subject matter. Email Aff. at ¶¶96-99.

II. *Argument.*

A. Relevant Legal Principles.

1. Warrants for Electronically Stored Information ("ESI").

Title 18, United States Code, § 2703 permits a government agent to "require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . ." 18 U.S.C. §2703(a). For contents stored for more than 180 days, a government agent may require the same disclosure by means of a court order, provided notice is given to the customer whose records are sought, or pursuant to a warrant when disclosure to a customer is not made. 18 U.S.C. §2703(b).

In 2009, Federal Rule of Criminal Procedure 41 was amended to include a procedure for warrants seeking electronically stored information. Under Rule

41(e)(2)(B), a warrant for electronically stored information "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information." The Committee notes to the 2009 amendment explain that subsection (e)(2) recognizes a two-step process in which "officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Significantly, the Committee also recognized the difficulties adapting the Fourth Amendment to modern technology, and cautioned, "[t]he amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development." Fed. R. Crim. P. 41, Committee Notes on Rules-2009 Amendment. The Committee Notes further recognized that "[i]ssues of particularity and search protocol are presently working their way through the courts," including, *inter alia*, "*United States v. Carey*, 172 F.3d 1268 (10th Cir.1999) (finding warrant authorizing search for 'documentary evidence pertaining to the sale and distribution of controlled substances' to prohibit opening of files with a .jpg suffix) and *United States v. Fleet Management Ltd.*, 521 F. Supp. 2d 436 (E.D. Pa. 2007) (warrant invalid when it 'did not even attempt to differentiate between data that there was probable cause to seize and data that was completely unrelated to any relevant criminal activity')."

2. Particularity.

As set forth in Mr. Merrill's companion motion, entitled "Defendant James Merrill's Motion to Suppress Evidence and Incorporated Memorandum of Law," the Fourth Amendment's particularity clause requires "that a valid warrant: (1) must supply

enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized." *United States v. Kuc*, 737 F.3d 129, 133 (1st Cir.2013). The primary purpose of the particularity requirement "is to prevent the use of general warrants authorizing wide-ranging rummaging searches in violation of the Constitution's proscription against unreasonable searches and seizures." *United States v. Logan*, 250 F.3d 350, 364-65 (6th Cir.), *cert. denied*, 534 U.S. 895, 997 (2001).

In every case, the descriptions of the items to be seized "must be as specific as the circumstances and the nature of the activity under investigation permit." *United States v. Greene*, 250 F.3d 471, 477 (6th Cir.2001). *See, e.g., Logan*, 250 F.3d at 365 (same). General descriptions will suffice only "[w]hen a more specific description of the items to be seized is unavailable." *United States v. Blakeney*, 942 F.2d 1001, 1026 (6th Cir.), *cert. denied*, 502 U.S. 1035 (1991). "The uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Groh v. Ramirez*, 540 U.S. 551, 559 (2004). While a magistrate's evaluation of an affidavit is accorded deference, *United States v. Jewell*, 60 F.3d 20, 22 (1st Cir.1995), "[that] [d]eference . . . is not boundless." *United States v. Leon*, 468 U.S. 897, 914 (1984). Such deference does not, for example, extend to permit the upholding of a warrant that fails to describe with particularity the items subject to seizure and which provides searching agents unfettered discretion in choosing what to seize. *See e.g., United States v. Fuccillo*, 808 F.2d 173, 176 (1st Cir.1987).

In addition, the scope of the search that may properly be authorized by the issuing judge may be no broader than the probable cause established by the affidavit. "An

otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based." *United States v. Leary*, 846 F.2d 592, 605 (10th Cir.1988). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). A warrant that authorizes a search for items as to which the affidavit fails to establish probable cause is overbroad and violates the Fourth Amendment. *See Leary*, 846 F.2d at 605 ("When the probable cause covers fewer documents in a system of files, the warrant must . . . tell the officers how to separate the documents to be seized from the others"). All items seized pursuant to an overbroad category are subject to suppression. *See United States v. Diaz*, 841 F.2d 1, 4 (1st Cir. 1988).

B. The Seizure Portion of the Email Warrant was Overbroad and Lacked Particularity.

In several cases decided since the 2009 amendment to Rule 41, several magistrate judges have issued strongly worded opinions in denying overbroad warrants seeking electronically stored information. In the case styled *In the Matter of the Search of the Premises known as: Three Hotmail accounts*, 2016 WL 1239916 (D.Kansas 2016), Magistrate Judge David J. Waxsie denied a § 2703 warrant seeking the same two-part "seize then search" process authorized by the warrant in this case. Specifically taking issue with the government's failure to consider a citizen's privacy rights in seeking an unlimited seizure of electronic communications, the Court explained:

This Court, however, continues to disagree with cases that find the

> proposed warrants were not overly broad in their authorization for the Email Provider to disclose—without limitation or any concern for the privacy rights of the account holder or any person communicating with that account—all ESI in or associated with the target email account.
>
> The chief aim of this Court's email (and cellular phone) opinions has been preventing the issuance of general warrants in the context of ESI. This Court has discussed the abhorrence of "general warrants," which were the chief evil the Framers were concerned with when drafting the Fourth Amendment. These days, courts discuss general warrants in boilerplate fashion: a quote or two in the legal standards section of an opinion, backed up with the same general case citations, and with the seemingly sole purpose of reiterating the fact that the court knows it should protect against general warrants. The problem with this framing is that the term "general warrants" fails to grasp courts' attention, having been beaten into rote regurgitation. Perhaps the time has come to reframe the discussion in terms of Americans' right to privacy.

Similarly, in *In re: [REDACTED]@gmail.com*, 62 F.Supp.3d 1100, 1104 (N.D.Cal. May 9, 2014), Magistrate Judge Paul Grewal denied a similar search warrant for email. The Court wrote:

> The court is nevertheless unpersuaded that the particular seize first, search second proposed here is reasonable in the Fourth Amendment sense of the word. On past occasions, the government at least submitted a date restriction. Here, there is no date restriction of any kind. The activity described in the application began in 2010; Gmail has been broadly available since 2007 and in beta release since 2004. Nor has the government made any kind of commitment to return or destroy evidence that is not relevant to its investigation. This unrestricted right to retain and use every bit Google coughs up undermines the entire effort the application otherwise makes to limit the obvious impact under the plain view doctrine of providing such unfettered government access.

Magistrate Judge Facciola in the District of Colombia has taken the analysis a step further:

> The problem here, as previously pointed out by this Court, is that the government is "abusing the two-step procedure under Rule 41" by requiring Apple to disclose the entire contents of an e-mail account. A seizure unquestionably occurs once data is turned over from Apple to the government. The government cannot pretend that the seizure only occurs after it has searched and separated the relevant e-mails from the irrelevant

> ones. And the two-step Rule 41 process, which has essentially created a narrow exception to the general prohibition against seizing data for which there is no probable cause, is permissible only because there is no alternative that would allow the government to access the data for which it does have probable cause. The Court must emphasize that the two-step procedure is a narrow exception that requires an affirmative showing of need in the warrant application. The Renewed Application, however, fails to provide any explanation for why the two-step procedure is necessary.
>
> . . .
>
> But this Court reaches this conclusion out of exasperation that the government has, despite repeated warnings, refused to determine an alternative that does not involve the wholesale seizure of vast amounts of e-mails and other data protected by the Fourth Amendment to which it has no right. Unless the government can suggest an appropriate alternative, the Court can only conclude that the Fourth Amendment does require that the provider perform the search because nothing else will eliminate the present certainty that the government will unconstitutionally seize data for which it has not established probable cause to seize.

In the Matter of the Search of Information Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F.Supp.3d 145, 147 (D.D.C April 7, 2013).

Other judges have disagreed. For example, in *In the Matter of a Warrant for all Content and Other Information Associated with Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F.Supp.3d 386 (S.D.N.Y. August 7, 2014) ("*S.D.N.Y Email*"), Magistrate Judge Gabriel W. Gorenstein issued a warrant for records from a Gmail account that was being used by a target of an investigation in furtherance of the alleged criminal activity. *S.D.N.Y Email*, 33 F.Supp.3d at 388. In defending his issuance of a two-part seize and search warrant, Judge Gorenstein cited to various court opinions upholding the off-site searching of a hard drive, explaining that he "perceive[d] no constitutionally significant difference between the searches of hard drives . . . and searches of email accounts" and "[t]he need to permit the Government to

examine electronic materials off-site rather than require it to conduct an on-site search is most obviously demonstrated in the case of a search of a computer hard disk drive . . . " *Id.* at 392.

In drawing the analogy, however, Judge Gorenstein ignores the obvious distinction between a law enforcement seizure and search of a hard drive and the seizure and search of ESI from a stored communications provider. In the case of a lawful seizure of a computer's hard drive, agents cannot limit their seizure to only a portion of the device without accessing and searching the drive. In the case of email in the custody of a stored communications provider, however, the government can easily limit the scope of their seizure before ever accessing the data, by simply restricting their request to a date range over which the alleged criminal conduct occurred. Despite authorizing a warrant unrestricted by any date range, Judge Gorenstein recognized the reasonableness of courts requiring the government to properly date restrict their request for stored communications. In addressing Judge Facciola's holding that the Fourth Amendment requires the stored communications provider to conduct the actual search protocol, Judge Gorenstein observed:

> There might be some force to requiring an email host to cull emails from an email account where a limitation in the scope of the items to be seized would allow the email host to produce responsive material in a manner devoid of the exercise of skill or discretion, for example, under a warrant requiring disclosure of all emails <u>from a particular time period</u>. But in the absence of such circumstances, it is unrealistic to believe that Google or any other email host could be expected to produce the materials responsive to categories listed in a search warrant.

Id. at 394 (emphasis added).

Mr. Merrill respectfully submits that, consistent with the opinions of a growing number of magistrate judges, in failing to properly date-restrict the email and data to be

seized from a stored communications provider, the government here offended the particularity requirement of the Fourth Amendment. The government had available to it the ability to balance its interest in seeking relevant evidence with the privacy interests of Mr. Merrill, by simply constraining its request to Comcast to the period of the alleged scheme. The government chose otherwise, deciding it was entitled to seek years' worth of email for which it did not have probable cause. Agent Soares' blatant disregard for the privacy interests of the person he was investigating is underscored by the failure of the affiant to date restrict the seizure despite his belief that probable cause existed for email only as far back as October 2012. *See* Exhibit 1, Category III.

In doing so, the affiant knowingly seized an excessive amount of email likely to contain personal and highly sensitive email communications between and among Mr. Merrill, his wife Kristin, his three children, his extended family, and close friends, none of whom were alleged to have participated in the criminal conduct. Just as troubling was the affiant's decision to seek email that post-dated Mr. Merrill's arrest, during which time Mr. Merrill was represented by counsel in his criminal case. In doing so, the affiant altogether ignored the sanctity of the attorney-client privilege and commanded the seizure of emails that were likely to contain attorney-client communications. This effort was particularly egregious because the affiant did not possess any information suggesting that Mr. Merrill was using his personal email account after his arrest to engage in obstructive or other criminal conduct. Indeed, the affidavit does not identify a single email that post-dated the arrest of Mr. Merrill for which there existed probable cause.

The sheer breadth of the seizure demand in this case is indicative of the affiant's abject disregard for the privacy interests of Mr. Merrill and his family, and emblematic of

the affiant's determination that he was not constrained by the requirements of probable cause and particularity in searching for evidence connected to the alleged pyramid scheme. In demanding the entire contents of Mr. Merrill's email account, the affiant requested potentially years' worth of email to rummage through for a scheme that was alleged to have lasted, at most, less than two years. The government here utterly failed to tailor its seizures to the proper justifications of its investigation, and the warrant thus took "on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. at 84.

C. The Search Portion of the Email Warrant was Overbroad.

The search protocol of the email warrant also fails the particularity test because its date restriction, which applied to every listed category in the warrant, authorized agents to search email from October 1, 2012, through September 25, 2014 (the date of the warrant's issuance). This time limitation unquestionably contravened the particularity requirement because the alleged criminal scheme ended, at the latest, on May 9, 2014, when Mr. Merrill was arrested. There was simply no justification for a search protocol that extended beyond the period for which probable cause existed and across a timeframe when Mr. Merrill was represented by counsel who was actively litigating Mr. Merrill's case. On the day of Mr. Merrill's arrest, an attorney was appointed to his case. *See* Dkt. Entry 4. On June 2, 2014, undersigned counsel entered an appearance on behalf of Mr. Merrill and on June 19, 2014, Mr. Merrill was released from custody. *See* Dkt. Entries 24, 49. Thus, the affiant had every reason to know that beginning on June 19, 2014, and continuing until the issuance of the email warrant on September 25, 2014, Mr. Merrill had access to his personal Comcast email account and would have been communicating

extensively with counsel. In addition, as discussed above, the affiant did not possess any information suggesting that Mr. Merrill was using his personal email account after his arrest to engage in obstructive or other criminal conduct. Yet, inexplicably, the affiant sought, and was improperly granted, authorization to search across Mr. Merrill's email account for this same period.

While all search protocols are necessarily overbroad in light of the improper date range, there are several other overbreadth issues with the search warrant. For example, Category 4 of the warrant authorized the searching of "all electronic data files," all videos, all "calendar data," and all "lists of friends, buddies contacts or other subscribers." There is no basis for the government to search "all electronic data files," without any limitation as to subject matter bearing some relationship to TelexFree. As written, the warrant would permit the seizure of a personal diary, a letter to Mr. Merrill's wife or child, or any other innumerable personal notes. The same is true for images, videos, calendars, and/or lists of friends. The expansive search protocol meant agents could seize and search diary entries relating to personal matters, such as medical appointments or political meetings, and /or photos or videos highly personal in nature, such as family vacations, personal moments, and/or video-diary entries. Likewise, Category 8 authorized the seizure and search of "[o]ther e-mail or Internet accounts," without any limitations. These expansive, unlimited categories illustrate the government's indifference to the privacy interests of Mr. Merrill and the bounds of the Fourth Amendment.

For these and the reasons set forth above, the search protocol of the email warrant was overbroad and insufficiently particular to satisfy the Fourth Amendment.

D. Leon does not Apply to the Warrant at Issue.

As set forth in the companion motions filed herewith, the government has the burden to demonstrate the applicability of the good faith exception first articulated in *United States v. Leon*, 468 U.S. 897, 923 (1984), and unless it can meet that burden, the evidence must be suppressed. *See, e.g., United States v. Diehl*, 276 F.3d 32, 42 (1st Cir. 2002). In the context of an overbroad warrant, "a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923.

The First Circuit has repeatedly declined to apply the good faith exception in circumstances where an affiant recklessly fails to distinguish items properly subject to seizure from those for which probable cause has not been established. *See e.g. United States v. Fuccillo*, 808 F.2d 173, 178 (1st Cir.1987) (declining to apply *Leon* where affiant failed to limit the search to stolen women's clothing for which probable cause existed and impermissibly broadened the scope of the warrant); *United States v. Roche*, 614 F.2d 6, 7-8 (1st Cir. 1980) (*Leon* does not apply where the government simply could have limited the search to automobile insurance records for which probable cause existed but declined to do so and impermissibly broadened the scope of the search); *In re Application of Lafayette Academy, Inc.*, 610 F.2d 1 (1st Cir.1979) (no good faith where government sought warrant for broad class of documents that should have been limited to meet the particularity requirement); *cf. United States v. Diaz*, 841 F.2d 1, 5-6 (1st Cir.1988) (good faith a "close call" where warrant permitted seizure of company's

records dating to inception of company, but first instance of identified fraud occurred eight months after company's inception).

Here, as in *Diaz*, the affiant sought records for a time period that extended beyond the period for which probable cause existed, but the *Leon* analysis in this case is not the close call it was in *Diaz*. In this case, the affiant extended the time period for which probable cause existed by many years, not eight months. Second, unlike *Diaz*, where the offending search concerned business records, in this case the Fourth Amendment violation resulted in the improper seizure and search of a personal Internet email account, a medium across which individuals share personal and often intimate details about their personal lives. Finally, the affiant's request to search Mr. Merrill's personal email for a period that post-dated his arrest and the alleged criminal activity and during which he was communicating with undersigned counsel was so offensive to the dictates of the Fourth Amendment that no reasonable law enforcement agent could have believed in the warrant's validity.

III. *Conclusion*.

For all of the reasons detailed herein, Mr. Merrill respectfully submits that all evidence seized pursuant to the email warrant must be suppressed.

Respectfully Submitted,
JAMES MERRILL,
By His Attorney,

/s/ Robert M. Goldstein
Robert M. Goldstein, Esq.
Mass. Bar No. 630584
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 742-9015

rmg@goldstein-lawfirm.com

Dated: May 20, 2016

Certificate of Service

I, Robert M. Goldstein, hereby certify that on this date, May 20, 2016, a copy of the foregoing document has been served via the Electronic Court Filing system on all registered participants, including Assistant U.S. Attorneys Andrew Lelling and Neil Gallagher.

/s/ Robert M. Goldstein